# CHAPTER 5
# RELIABILITY CONSIDERATIONS

## 5-1. Reliability criteria

Mechanical and electrical support systems for C4ISR facilities are required to be designed to attain a reliability/availability (R/A) of 0.999999. SCADA systems are integral to the function of the mechanical and electrical support systems and must therefore be designed to support this R/A goal. A mechanical/electrical system configuration that meets this criterion based on analysis of the process flow diagram or the electrical one-line will not achieve it if the control system compromises the reliability/availability designed into the process.

a. *Reliability* defines the probability of a system serving its function or being able to perform its mission over a certain fixed period of time. A system having a reliability of 0.999999 for a specific mission time has a 99.9999% chance of functioning without failure over that period.

b. *Availability* defines the long-term fraction of time that a system is functioning properly or able to perform its mission. A system with availability of 0.999999 will have an average downtime of only 31 seconds per calendar year. This does NOT mean that the average outage of the system will last 31 seconds; it only means that the number of expected failures per year multiplied by the average outage length equals 31 seconds per year. For example, a probability of a failure occurring once every 40 years, with an average duration of 20 minutes, would be more typical of a facility with an availability of 0.999999. Given their continuous operation and lack of a defined mission time, availability is generally a more appropriate design criterion than reliability for SCADA systems.

## 5-2. Reliability calculations

If the time, t, over which a system must operate and the underlying distributions of failures for its constituent elements are known, then the system reliability can be calculated by taking the integral (essentially the area under the curve defined by the failure distribution) from t to infinity, as shown in equation 5-1.

$$R(t) = \int_t^\infty f(t)\,dt \qquad \text{(Equation 5-1)}$$

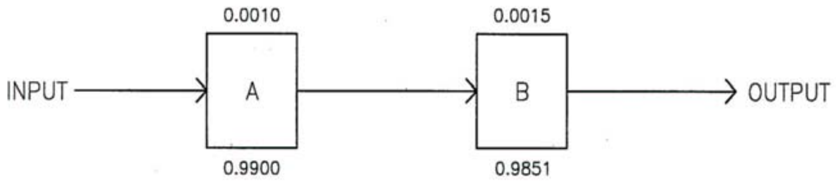
a. *Exponential distribution*. If the underlying failure distribution is exponential, a common, but only approximate, assumption for mechanical and electrical systems, equation 5-1 becomes equation 5-2. If the underlying distribution for each element is exponential and the failure rates, $\lambda_i$, for each element are known, then the reliability of the system can be calculated using equation 5-2.

$$R(t) = e^{-\lambda t} \qquad \text{(Equation 5-2)}$$

where:

$\lambda$ is the failure rate
*t* is the length of time the system must function
*e* is the base of natural logarithms
R(t) is reliability over time *t*

b. *Series reliability*. Consider the system represented by the reliability block diagram (RBD) in figure 5-1.



NOTES:

1. THE NUMBER ABOVE EACH BLOCK IS THE FAILURE RATE IN FAILURES PER HOUR.
2. THE NUMBER BELOW EACH BLOCK IS THE RELIABILITY CALCULATED USING EQUATION 5-2 WITH T = 10 HOURS (EXPONENTIAL DISTRIBUTION ASSUMED).

*Figure 5-1. Reliability block diagram.*

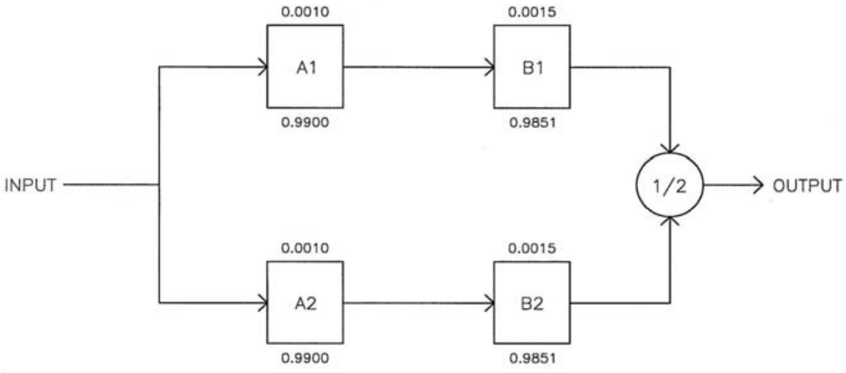
(1) *Series configuration - the weakest link*. A and B in figure 5-1 are said to be in series, which means all must operate for the system to operate. Since the system can be no more reliable than the least reliable component, this configuration is often referred to as the weakest link configuration. An analogy would be a chain; the strength of the chain is determined by its weakest link.

(2) *Series calculation method 1*. Since the components are in series, the system reliability can be found by adding together the failure rates of the components and substituting the result in equation 5-2. The system failure rate is 0.001000 + 0.001500 = 0.002500. The reliability is:

$$R(t) = e^{-0.0025x10} = 0.9753 \qquad \text{(Equation 5-3)}$$

(3) *Series calculation method 2*. Alternatively, we could find the system reliability by multiplying the reliabilities of the two components as follows: 0.9900 x 0.9851 = 0.9753.

c. *Reliability with Redundancy*. Now consider the RBD shown in figure 5-2.



NOTES:

3. THE NUMBER ABOVE EACH BLOCK IS THE FAILURE RATE IN FAILURES PER HOUR.

4. THE NUMBER BELOW EACH BLOCK IS THE RELIABILITY CALCULATED USING EQUATION 5-2 WITH T = 10 HOURS (EXPONENTIAL DISTRIBUTION ASSUMED).

*Figure 5-2. RBD of a system with redundant components.*

(1) *The redundant or parallel configuration.* The system represented by the RBD in figure 5-2 has the same components (A and B) used in figure 5-1, but two of each component are used in a configuration referred to as redundant or parallel. Two paths of operation are possible. The paths are top A-B and bottom A-B. If either of two paths is intact, the system can operate. The reliability of the system is most easily calculated by finding the probability of failure (1 - R (t)) for each path, multiplying the probabilities of failure (which gives the probability of both paths failing), and then subtracting the result from 1. The reliability of each path was found in the previous example. Next, the probability of a path failing is found by subtracting its reliability from 1. Thus, the probability of either path failing is 1 - 0.9753 = 0.0247. The probability that both paths will fail is 0.0247 x 0.0247 = 0.0006. Finally, the reliability of the system is 1 - 0.0006 = 0.9994, about a 2.5% improvement over the series-configured system.

(2) *Types of redundancy.* Two components in parallel (redundant) may always be on and in operation (hot standby) or one may be off or not in the "circuit" (cold standby). In the latter case, failure of the primary component must be sensed and the standby component turned on or switched into the circuit. Standby redundancy may be necessary to avoid interference between the redundant components and, if the redundant component is normally off, reduces the time over which the redundant component will be used (it's only used from the time when the primary component fails to the end of the mission). Of course, more than two components can be in parallel. Both types of standby redundancy are available in PLC systems

## 5-3. Redundancy terminology

Redundant configurations of systems and equipment are commonly referred to using mathematical formulas based on the parameter "N", such as "N + 1" or "2N". In this convention, N is the number of systems or pieces of equipment which must be operational to meet the load or accomplish the mission.

a. N + X redundancy refers to a system configuration in which the total number of units provided is equal to the number needed to meet the load, N, plus some number of spare units, X. For example, if a cooling system requires 300 gallons per minute (gpm) of flow, and five 100 gpm pumps are provided, the system would be described as N + 2, where N = 3.

b. XN redundancy refers to a system configuration in which the total number of units provided is some multiple, X, of the number required to meet the load. For example, if the same cooling system were provided with two 300 gpm pumps, it would be described as 2N, where N = 1.

Further information on redundant system configurations can be obtained from TM 5-698-1 – Reliability/Availability of Electrical and Mechanical Systems for Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) Facilities.

## 5-4. Availability calculations

a. Once an expected failure rate, λ, is known for a component or a system, the associated availability can be calculated from the failure rate and the repair time, *r* as in equation 5-4.

$$A = \frac{8760 - \lambda r}{8760} \qquad \text{(Equation 5-4)}$$

λ = failure rate, per year
*r* = repair time, hours

b. Availability can also be calculated from published or tested Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR) data using equation 5-5:

$$A_i = \frac{MTBF}{MTBF + MTTR} \times 100\% \qquad \text{(Equation 5-5)}$$

Availability calculated on this basis is also termed *inherent availability*, $A_i$, as it is based only on the inherent failure characteristics of the system and does not account for unavailability for scheduled maintenance or overhauls. *Operational availability*, $A_o$, is availability calculated including the effects of scheduled downtime based on Mean Time Between Maintenance (MTBM) and Mean Down Time (MDT) as shown in Equation 5-6. As SCADA systems and components rarely require extended shutdowns for maintenance, inherent availability is an appropriate design and performance criteria.

$$A_o = \frac{MTBM}{MTBM + MDT} \times 100\% \qquad \text{(Equation 5-6)}$$

## 5-5. Component reliability

The components used to assemble SCADA systems are typically industrial- or utility-grade sensors, controllers, relays and actuators, which are mass-produced in large numbers for the commercial market and generally are not designed to Military Specifications (MilSpec) or to documented reliability criteria. Where available, SCADA systems should use components meeting the applicable MilSpec designations. For those applications where such components are not available, components should comply with other applicable industry standards that address reliability, maintainability, environmental protection, seismic withstand, surge withstand, etc.

a. Reliability of non-Milspec components should be enhanced by specifying heavy-duty components or overrating of devices, where such overrating does not interfere with the operation or function of the component. Examples include:

(1) Use of 600V rated wire for all control circuits operating above 50 V.

(2) Use of relays with contact ratings exceeding circuit voltage and current ratings in power circuits.

(3) Derating of devices to operate below a specified fraction (often 80%) of their capability.

b. Reliability data for electrical components used in the power supply circuits for SCADA systems can be obtained from IEEE 493, also known as “The Gold Book” or from the PREP Equipment Reliability Database.

## 5-6. Systems reliability

Reliability of a SCADA system can be calculated from the known indices of the components or subsystems as described above. From a qualitative standpoint, however, there are two primary considerations in developing a reliable SCADA system: Providing segregation and redundancy corresponding to that specified for the supported mechanical and electrical systems; and keeping the configuration, control sequences, and programming as simple as is consistent with the required functionality. The tendency to design control sequences to account on an automatic basis for every conceivable contingency or to provide sustained service to the load after the third or fourth contingency failure often results in systems that are unwieldy to operate and makes it difficult for operators to retain knowledge of the system. Because of the critical role of humans in the function of SCADA systems (see chapter 6), complex configurations and sequences that provide very high calculated reliability/availability indices may actually produce significantly lower real-world availability than simpler systems due to the effects of human action.

a. It is said that *software* neither fails randomly nor wears out, and thus all software failures must be designed into the system, and simply remain dormant until the right combination of input conditions, timing and logic cause them to show up. SCADA software should incorporate self-diagnostic features including flow control, watchdog timers, and reasonableness checking. Failure of a self-diagnostic check should result in an alarm report to the supervisory system, driving all outputs to a defined fail-safe state, and transfer of control to the redundant processor, where provided. Comprehensive commissioning testing, as described in chapter 8, can significantly reduce the likelihood of undiscovered software errors.

b. System reliability can be enhanced by anticipating likely *field device* failure modes and providing program logic to detect them. For example, monitoring the position of a critical circuit breaker using only a single normally open or normally closed auxiliary contact leaves the control system vulnerable to false information in the event of a short or open on the input circuit. If both contacts are used, they must always agree on the state of the breaker, or a faulted input circuit is declared and automatic operation of that breaker suspended.

## 5-7. Power supply sources

The preferred power supply for SCADA systems is the direct current (DC) station battery system supplying the equipment controlled by the SCADA. DC Station battery systems can be inherently more reliable than alternating current (AC) uninterruptible power supply (UPS) systems, because they rely on electronic components only to maintain the batteries in a charged state, and not to deliver energy to the load. PLCs are available with DC power supplies rated at voltages between 24 VDC and 125 VDC, and DC-DC converters are available to supply lower voltage components from higher voltage systems.

a. Station battery banks provide voltage over a range limited on the lower end by the specified end-of-discharge voltage, which is typically 1.75 volts per cell (VPC) for lead-acid batteries and 1.14 VPC for nickel cadmium batteries and on the upper end by charging voltage required to periodically equalize the batteries, typically 2.38 VPC for lead-acid and 1.70 VPC for nickel cadmium. SCADA components must be rated to operate properly over this range, or must be provided with DC-DC converters that are rated for this input range.

b. The level of redundancy in power supply circuits should correspond to the redundancy criteria of the PLC. For example, in multiple generator paralleling switchgear applications where reliability is attained through an N+X generator configuration, it is common for each generator to be provided with a single PLC supplied from the DC control voltage source of that generator, which is typically the starting battery. A redundant power circuit to the generator PLC would add no benefit as the generator cannot start without local control power anyway. The master controller associated with the paralleling switchgear, however, is typically a redundant PLC configuration. It should be provided with redundant DC supplies from separate station battery banks.

c. Diode-based “best battery” selection systems, as shown in figure 5-3 may be used to increase system availability by supplying non-redundant pieces of switchgear or SCADA system equipment from two or more DC power sources. This arrangement provides automatic protection against low voltage or complete loss of one source, as the diode pair with the highest voltage is always conducting and the “failed” source is isolated from the load by the other diode pair that is in a reverse-biased blocking state. This source selection scheme must only be used at the branch circuit level, as it does not provide isolation of the sources for short circuits on the load side of the diodes. Such a short circuit will cause both diodes to conduct, clearing the fuses or tripping the circuit breakers on both DC circuits. For this reason, individual sets of diodes should be provided for each PLC cabinet, circuit breaker, etc. to limit the outage to the affected unit.

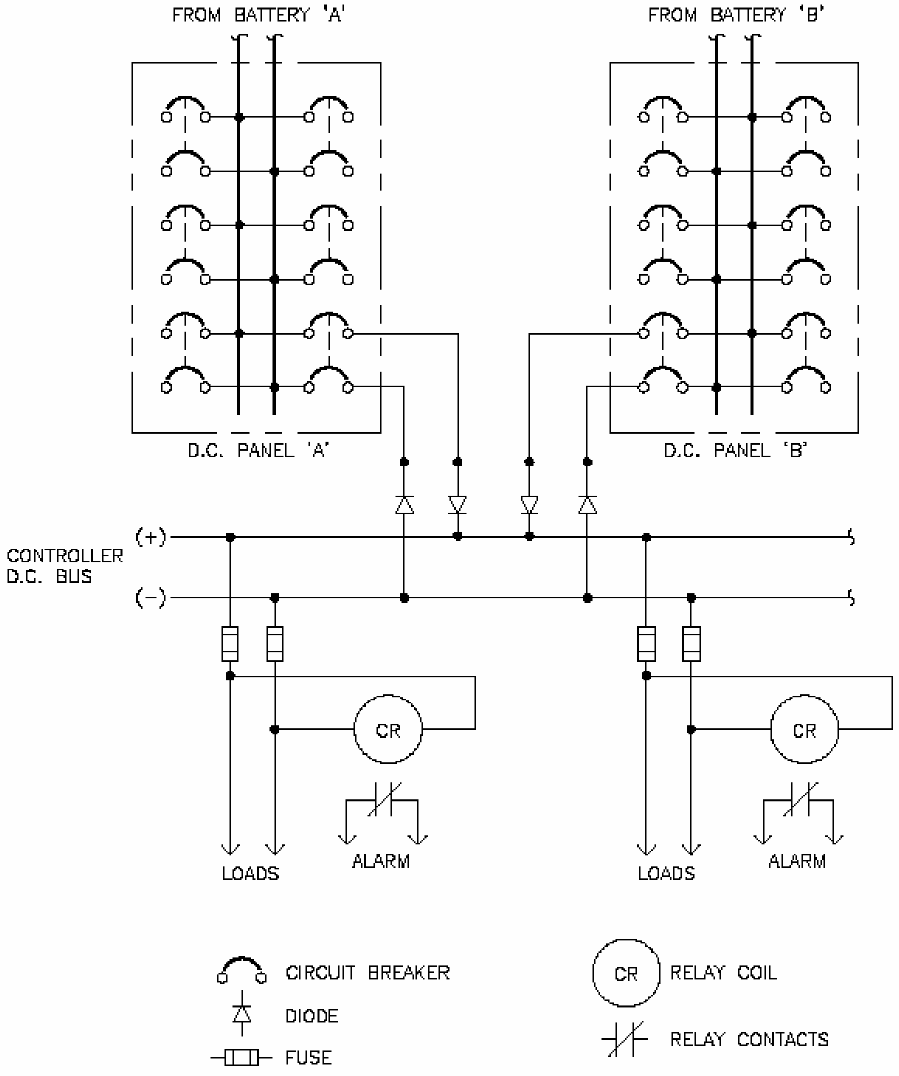


*Figure 5-3. Diode-based "best-battery" selector circuit*

d. Every branch of a control power circuit should be provided with a voltage relay or other means of supervision to verify continuously the presence of control power. This supervision should be provided on the load side of all fuses, circuit breakers, diodes and transfer switches. Failure of any control power branch circuit should initiate local and central alarms.

e. Where UPS systems must be used to supply SCADA equipment that requires AC power, they should be of the on-line, or reverse transfer type, in which the rectifier-inverter combination is normally supplying the load while float-charging the battery and provided with quarter-cycle static switching to the AC line upon inverter failure. UPS systems should be selected in compliance with TM 5-693, Uninterruptible Power Supply System Selection, Installation, and Maintenance for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities.

f. SCADA power supplies must be provided with overcurrent protective devices (fuses or circuit breakers) whose ratings and settings have been determined to provide selectively coordinated protection. Selective coordination is defined as opening the protective device closest to the point of the fault without opening upstream devices, thus limiting the associated outage to the faulted circuit or equipment. Guidelines for selective coordination can be found in IEEE 242 – Protection and Coordination of Industrial Power Systems.

## 5-8. Segregation

Redundant components and subsystems should be segregated electrically and physically to reduce the probability of common mode failure from electrical, environmental, or physical threats.